PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-165728
(43)Date of publication of application : 02.07.1993

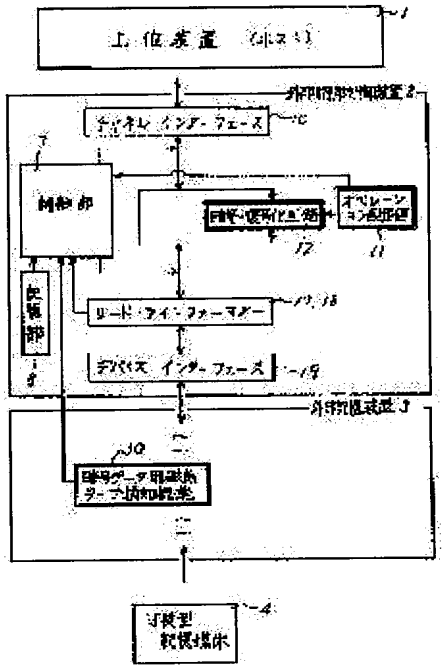
(51)Int.Cl. G06F 12/14
G06F 3/06

(21)Application number : 03-333283
(22)Date of filing : 17.12.1991

(71)Applicant : FUJITSU LTD
(72)Inventor : TAKAI NOBUYUKI
KAGAWA KENJI

(54) EXTERNAL STORAGE SUB-SYSTEM

(57)Abstract:
PURPOSE: To facilitate the introduction of an external storage sub-system without giving burden on a host device for a ciphering/decoding processing on the external storage sub-system which ciphers and decodes data through the use of an exchangeable storage medium such as a magnetic tape.
CONSTITUTION: The external storage sub-system where an external storage device 3 which writes/reads data in the exchangeable storage medium 4 and an external storage controller 2 controlling the external storage device 3 are given, the external storage controller 2 connected to the host device 1 controls the external storage device 3, write data from the host device 1 is written into the exchangeable storage medium 4, data from the exchangeable storage medium 4 is read and it is transferred to the host device 1 which is provided with a ciphering/decoding circuit 12 which ciphers write data from the host device 1 and decodes read data from the external storage device 3 for the external storage controller 2.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－165728

(43)公開日　平成５年(1993)７月２日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｂ	9293－5B		
3/06	３０４　Ｈ	7165－5B		

審査請求　未請求　請求項の数５(全　８　頁)

(21)出願番号　特願平3－333283

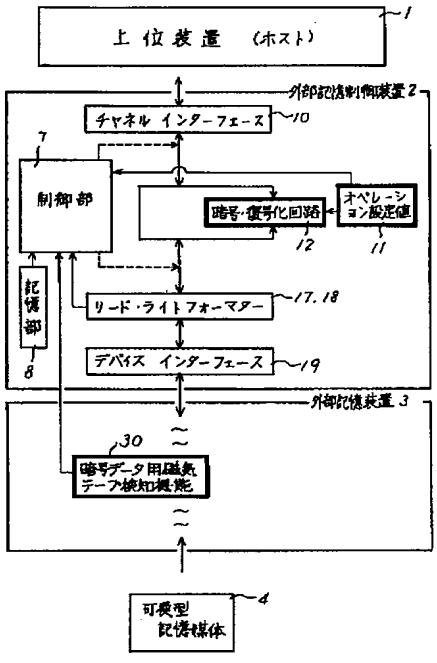
(22)出願日　平成３年(1991)12月17日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　高井　伸幸
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　香川　謙治
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　山谷　晧榮

(54)【発明の名称】　外部記憶サブシステム

(57)【要約】
【目的】　磁気テープ等の可換型記憶媒体を用いて、データを暗号化・復号化する外部記憶サブシステムに関し、暗号化・復号化処理に上位装置の負担にならずに、且つ導入がし易いことを目的とする。
【構成】　可換型記憶媒体４の書き込み／読み出しを行う外部記憶装置３と、該外部記憶装置３を制御する外部記憶制御装置２とを有し、上位装置１に接続された該外部記憶制御装置２が該外部記憶装置３を制御して、該可換型記憶媒体４に該上位装置１からの書き込みデータを書き込み、該可換型記憶媒体４からのデータを読み出して、該上位装置１への転送を行う外部記憶サブシステムにおいて、該外部記憶制御装置２に、該上位装置１からの書き込みデータを暗号化し、該外部記憶装置３からの読み出しデータを復号化する暗号化・復号化回路１２を設けた。

本発明の原理図



1

【特許請求の範囲】
【請求項１】　可換型記憶媒体（４）の書き込み／読み出しを行う外部記憶装置（３）と、該外部記憶装置（３）を制御する外部記憶制御装置（２）とを有し、上位装置（１）に接続された該外部記憶制御装置（２）が該外部記憶装置（３）を制御して、該可換型記憶媒体（４）に該上位装置（１）からの書き込みデータを書き込み、該可換型記憶媒体（４）からのデータを読み出して、該上位装置（１）への転送を行う外部記憶サブシステムにおいて、
該外部記憶制御装置（２）に、該上位装置（１）からの書き込みデータを暗号化し、該外部記憶装置（３）からの読み出しデータを復号化する暗号化・復号化回路（１２）を設けたことを特徴とする外部記憶サブシステム。
【請求項２】　前記外部記憶装置（３）に、前記可換型記憶媒体（４）が暗号用であることを検出する記憶媒体検出手段（３０）を設けるとともに、前記外部記憶制御装置（２）に、前記記憶媒体検出手段（３０）の検出内容に応じて、前記暗号化・復号化回路（１２）を制御する制御部（７）を設けたことを特徴とする請求項１の外部記憶サブシステム。
【請求項３】　前記外部記憶制御装置（２）に、上位装置（１）からの命令により、前記暗号化・復号化回路（１２）を制御する制御部（７）を設けたことを特徴とする請求項１の外部記憶サブシステム。
【請求項４】　前記外部記憶制御装置（２）は、前記外部記憶装置（３）からの読み出しデータにより、暗号化データであるかを判定する判定手段（１７）を有することを特徴とする請求項２又は３の外部記憶サブシステム。
【請求項５】　前記外部記憶制御装置（２）に、前記暗号化・復号化回路（１２）の暗号化情報を設定する設定部（１１）を設けたことを特徴とする請求項１又は２又は３又は４の外部記憶サブシステム。
【発明の詳細な説明】
【０００１】（目次）
産業上の利用分野
従来の技術（図４）
発明が解決しようとする課題
課題を解決するための手段（図１）
作用
実施例
(a) 一実施例の説明（図２乃至図３）
(b) 他の実施例の説明
発明の効果
【０００２】
【産業上の利用分野】本発明は、磁気テープ等の可換型記憶媒体を用いて、データを暗号化・復号化する外部記憶サブシステムに関する。
【０００３】近年のコンピュータシステムの発展に伴い、外部記憶装置の重要機密情報の保護が問題となっているが、磁気テープ、磁気ディスク、光ディスク等の交換可能な可換型記憶媒体は、可換型のため、盗難が可能であり、盗難されると簡単に読み込まれ、データが漏洩してしまう。

2

【０００４】この重要機密情報のセキュリティの強化の要求に伴い、漏洩防止策として、コンピュータ室の入室管理を強化する方法では、盗難の危険性が皆無と言えず、盗難されても読めないように、書き込みデータを暗号化して記録し、読み出しデータを復号化する方法が提供されており、コンピュータシステムに導入し易いものが望まれている。
【０００５】
【従来の技術】図４は従来技術の説明図である。図４に示すように、磁気テープカートリッジ４を用いた外部記憶サブシステムは、ホスト（上位装置）１と接続された磁気テープ制御装置２と、磁気テープ制御装置２に制御され、磁気テープカートリッジ４に、ホスト１の書き込みデータを書き込み、データを読み出す磁気テープ装置３とを有する。
【０００６】このようなシステムにおいて、暗号化を行うため、従来ホスト１に、暗号化・復号化プログラムを設け、ホスト１が、必要なデータを当該プログラムによって、暗号化し、ライトデータを作成して、磁気テープ制御装置２に転送し、磁気テープ装置３を介し磁気テープ４に書き込み、磁気テープ４から読み取った暗号化データは、磁気テープ装置３より磁気テープ制御装置２を介しホスト１へ転送し、ホスト１の当該プログラムにより、復号化して、データ処理していた。
【０００７】
【発明が解決しようとする課題】しかしながら、従来技術では、次の問題があった。
①暗号化・復号化をホスト１のプログラムで実行するため、処理速度が遅いため、外部記憶の入出力処理全てが遅くなる他に、ホスト１の負担がかかり、ホストの処理能力低下をきたすおそれがあった。
【０００８】②ホストの既存の外部記憶の入出力処理全てに、暗号化・復号化機能を追加する作業が必要となり、作業量（工数）が多く、暗号化・復号化機能導入に長時間が必要となる。
【０００９】③ホストのプログラムは、人為的に作成するため、処理に誤り及び抜けがあると、外部記憶のデータ破壊及び処理障害が生じる。
④暗号化・復号化機能導入後も、新規の記憶媒体の入出力処理にも、暗号化・復号化機能を追加する作業が必要となるため、全体的な運用工数が増加する。
【００１０】⑤暗号化・復号化機能を追加するに当たり、記憶媒体上のデータが、暗号データか通常データかを判定する機能を新規に作成する必要がある。
従って、本発明は、暗号化・復号化処理に上位装置の負

担にならずに、且つ導入がし易い外部記憶サブシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】図１は本発明の原理図である。本発明の請求項１は、可換型記憶媒体４の書き込み／読み出しを行う外部記憶装置３と、該外部記憶装置３を制御する外部記憶制御装置２とを有し、上位装置１に接続された該外部記憶制御装置２が該外部記憶装置３を制御して、該可換型記憶媒体４に該上位装置１からの書き込みデータを書き込み、該可換型記憶媒体４からのデータを読み出して、該上位装置１への転送を行う外部記憶サブシステムにおいて、該外部記憶制御装置２に、該上位装置１からの書き込みデータを暗号化し、該外部記憶装置３からの読み出しデータを復号化する暗号化・復号化回路１２を設けたことを特徴とする。

【００１２】本発明の請求項２は、請求項１において、前記外部記憶装置３に、前記可換型記憶媒体４が暗号用であることを検出する記憶媒体検出手段３０を設けるとともに、前記外部記憶制御装置２に、前記記憶媒体検出手段３０の検出内容に応じて、前記暗号化・復号化回路１２を制御する制御部７を設けたことを特徴とする。

【００１３】本発明の請求項３は、請求項１において、前記外部記憶制御装置２に、上位装置１からの命令により、前記暗号化・復号化回路１２を制御する制御部７を設けたことを特徴とする。

【００１４】本発明の請求項４は、請求項２又は３において、前記外部記憶制御装置２は、前記外部記憶装置３からの読み出しデータにより、暗号化データであるかを判定する判定手段１７を有することを特徴とする。

【００１５】本発明の請求項５は、請求項１又は２又は３又は４において、前記外部記憶制御装置２に、前記暗号化・復号化回路１２の暗号化情報を設定する設定部１１を設けたことを特徴とする。

【００１６】

【作用】本発明の請求項１では、外部記憶制御装置２に、該上位装置１からの書き込みデータを暗号化し、該外部記憶装置３からの読み出しデータを復号化する暗号化・復号化回路１２を設けたので、上位装置１に、暗号化・復号化機能は不要となるので、上位装置の負担とならず、上位装置の入出力処理の遅れも防止でき、上位装置の既存処理の変更が必要なく、導入を短時間でで き、ハード回路で構成しているので、高速処理が可能となり、しかも誤り、障害によりデータ破壊等を防止できる。

【００１７】本発明の請求項２では、外部記憶装置３に、前記可換型記憶媒体４が暗号用であることを検出する記憶媒体検出手段３０を設けるとともに、前記外部記憶制御装置２に、前記記憶媒体検出手段３０の検出内容に応じて、前記暗号化・復号化回路１２を制御する制御部７を設けたので、書き込みデータを暗号化するかどうか、読み出しデータを復号化するかどうかを、セットされた可換型記憶媒体により判断できる。

【００１８】本発明の請求項３では、外部記憶制御装置２に、上位装置１からの命令により、前記暗号化・復号化回路１２を制御する制御部７を設けたので、書き込みデータを暗号化するかどうか、読み出しデータを復号化するかどうかを、上位装置１の命令により判断できる。

【００１９】本発明の請求項４では、外部記憶制御装置２は、前記外部記憶装置３からの読み出しデータにより、暗号化データであるかを判定する判定手段１７を有するので、読み出しデータにより、暗号化データが自動的に判断できる。

【００２０】本発明の請求項５では、外部記憶制御装置２に、前記暗号化・復号化回路１２の暗号化情報を設定する設定部１１を設けたので、ＤＥＳ、ＨＡＳＨ等の暗号方法や暗号キーを、運用に応じて設定できる。

【００２１】

【実施例】

(a) 一実施例の説明

図２は本発明の一実施例構成図、図３は本発明の一実施例説明図であり、磁気テープサブシステムを示している。

【００２２】図中、図１及び図４で示したものと同一のものは、同一の記号で示してあり、図２において、磁気テープ制御装置２は、ホストインターフェースコントロール部５と、フォーマットコントロール部６とで構成されている。

【００２３】１０はチャネルインターフェース部であり、ホスト（上位装置）１のチャネル１ａとのインターフェース制御を行うもの、１１はオペレーション設定部であり、オペレータが設定した暗号方法（ＤＥＳ、ＨＡＳＨ等）と暗号キーとを設定しておくもの、１２は暗号・復号化回路であり、制御部７からの制御により、設定された暗号方法・暗号キーで、書き込みデータを暗号化し、読み出しデータを復号化するもの、１３は圧縮・伸長化回路であり、制御部７からの制御により、書き込みデータ（又は暗号化された書き込みデータ）をデータ圧縮し、読み出しデータをデータ伸長するものである。

【００２４】１４はインターナルバスアダプタであり、内部（インターナル）バス２０へデータを送出し、内部バス２０のデータを取り込むもの、１５はマルチブロックバッファであり、ホストインターフェースコントロール部５側とフォーマットコントロール部６側とのデータ転送速度の吸収のため、データをバッファリングするもの、１６はインターナルバスアダプタであり、内部（インターナル）バス２０へデータを送出し、内部バス２０のデータを取り込むものである。

【００２５】１７はリードフォーマター部であり、磁気テープ装置３からのフォーマッティングされているリードデータを分析し、暗号データ、非暗号データ又は圧縮

データ又は非圧縮データであるかを判断し、その結果を制御部７に通知し、磁気テープ用にフォーマッティングされたリードデータをホスト用データに変換して、ホストインターフェースコントロール部５側に出力するもの、１８はライトフォーマター部であり、ライトデータを磁気テープ用にフォーマッティングし、磁気テープ装置３方向に出力するもの、１９はデバイスインターフェース部であり、磁気テープ装置３と磁気テープ制御装置２との間のデータの入出力制御、入出力処理を行うものである。

【００２６】７は制御部であり、マイクロプロセッサ（ＭＰＵ）で構成され、ライトデータの暗号化、非暗号化を判断し、圧縮化、非圧縮化を判断し、各部をライト制御し、リードデータの復号化、非復号化、伸長化、非伸長化を判断し、各部をリード制御するものであり、８は記憶部であり、コントロールストレージを構成し、制御部７が実行する制御プログラム等を格納するものである。

【００２７】磁気テープ装置３は、磁気テープドライブ装置で構成され、暗号、圧縮テープ検出機構３０を有し、セットされた磁気テープカートリッジ４のリード／ライトを行うものである。

【００２８】暗号、圧縮テープ検出機構３０は、図３に示すように、磁気テープカートリッジ４に設けた暗号シールＳ１を検出する暗号センサ３０ａと、磁気テープカートリッジ４に設けた圧縮シールＳ２を検出する圧縮センサ３０ｂとを有する。

【００２９】尚、磁気テープ４には、図３（Ｂ）に示すように、暗号フラグと圧縮フラグが先頭に設けられており、暗号フラグがセットされていると、暗号データが書き込まれている、圧縮フラグがセットされていると、圧縮データが書き込まれていると判断できるようにしている。

【００３０】磁気テープドライブ装置３に、磁気テープカートリッジ４がセットされると、暗号・圧縮テープ検出機構３０のセンサ３０ａ、３０ｂの出力を、制御部７に通知する。

【００３１】これにより、制御部７は、セットされた磁気テープカートリッジ４が、暗号・圧縮用か、暗号・非圧縮用か、非暗号・圧縮用か、非暗号・非圧縮用かを判定する。

【００３２】次に、ライト動作について説明する。ホスト１からライトアクセスがあると、チャネルインターフェース制御部１０を介して制御部７に通知され、ライト処理が起動される。

【００３３】制御部７は、磁気テープカートリッジ４が、非暗号・非圧縮テープであれば、ホスト１からのライトデータをチャネルインターフェース制御部１０を介し、インターナルバスアダプタ１４に直接転送し、バス２０、マルチブロックバッファ１５よりインターナルバスアダプタ１６に入力し、ライトフォーマター部１８で磁気テープ用にフォーマッティングし、デバイスインターフェース部１９より、磁気テープドライブ装置３に転送し、磁気テープカートリッジ４に書き込む。

【００３４】一方、磁気テープカートリッジ４が、暗号・非圧縮テープであれば、制御部７は、オペレーション設定部１１の暗号方法情報と暗号キーとにより、暗号・復号化回路１２を起動し、ホスト１からのライトデータをチャネルインターフェース制御部１０を介し、暗号・復号化回路１２に入力し、設定した暗号方法と暗号キーにより暗号データに変換して、インターナルバスアダプタ１４に転送し、バス２０、マルチブロックバッファ１５よりインターナルバスアダプタ１６に入力し、ライトフォーマター部１８で磁気テープ用にフォーマッティングし、デバイスインターフェース部１９より、磁気テープドライブ装置３に転送し、磁気テープカートリッジ４に書き込む。

【００３５】又、磁気テープカートリッジ４が、暗号・圧縮テープであれば、制御部７は、オペレーション設定部１１の暗号方法情報と暗号キーとにより、暗号・復号化回路１２を起動し、圧縮・伸長化回路１３を起動して、ホスト１からのライトデータをチャネルインターフェース制御部１０を介し、暗号・復号化回路１２に入力し、設定した暗号方法と暗号キーにより暗号データに変換した後、圧縮・伸長化回路１３に入力し、圧縮データに変換して、インターナルバスアダプタ１４に転送し、バス２０、マルチブロックバッファ１５よりインターナルバスアダプタ１６に入力し、ライトフォーマター部１８で磁気テープ用にフォーマッティングし、デバイスインターフェース部１９より、磁気テープドライブ装置３に転送し、磁気テープカートリッジ４に書き込む。

【００３６】更に、磁気テープカートリッジ４が、非暗号・圧縮テープであれば、制御部７は、圧縮・伸長化回路１３を起動して、ホスト１からのライトデータをチャネルインターフェース制御部１０を介し、圧縮・伸長化回路１３に入力し、圧縮データに変換して、インターナルバスアダプタ１４に転送し、バス２０、マルチブロックバッファ１５よりインターナルバスアダプタ１６に入力し、ライトフォーマター部１８で磁気テープ用にフォーマッティングし、デバイスインターフェース部１９より、磁気テープドライブ装置３に転送し、磁気テープカートリッジ４に書き込む。

【００３７】次に、リード動作について説明する。ホスト１からリードアクセスがあると、チャネルインターフェース制御部１０を介して制御部７に通知され、リード処理が起動される。

【００３８】制御部７は、磁気テープドライブ装置３からの磁気テープカートリッジ４のリードデータをデバイスインターフェース制御部１９を介し、リードフォーマター部１７に入力し、暗号フラグ、圧縮フラグの分析を

行わしめ、分析結果を受ける。

【００３９】リードフォーマター部１７はリードデータをホスト用のデータに直して、インターナルバスアダプタ１６に転送し、バス２０、マルチブロックバッファ１５よりインターナルバスアダプタ１４に入力する。

【００４０】制御部７は、分析結果により、リードデータが、非暗号・非圧縮であれば、インターナルバスアダプタ１４のリードデータを、チャネルインターフェース部１０に直接転送して、ホスト１に転送する。

【００４１】一方、制御部７は、分析結果により、リードデータが、暗号・非圧縮であれば、オペレーション設定部１１の暗号方法情報と暗号キーとにより、暗号・復号化回路１２を起動し、インターナルバスアダプタ１４のリードデータを、暗号・復号化回路１２に転送し、指定された暗号方法と暗号キーとにより複合データに変換せしめ、チャネルインターフェース部１０に転送して、ホスト１に転送する。

【００４２】又、制御部７は、分析結果により、リードデータが、暗号・圧縮テープであれば、制御部７は、オペレーション設定部１１の暗号方法情報と暗号キーとにより、暗号・復号化回路１２を起動し、圧縮・伸長化回路１３を起動して、インターナルバスアダプタ１４のリードデータを、圧縮・伸長化回路１３に転送して、伸長データに変換した後、暗号・復号化回路１２に転送し、指定された暗号方法と暗号キーとにより復号データに変換せしめ、チャネルインターフェース部１０に転送して、ホスト１に転送する。

【００４３】更に、制御部７は、分析結果により、リードデータが、非暗号・圧縮テープであれば、圧縮・伸長化回路１３を起動して、インターナルバスアダプタ１４のリードデータを、圧縮・伸長化回路１３に転送して、伸長データに変換した後、チャネルインターフェース部１０に転送して、ホスト１に転送する。

【００４４】このようにして、磁気テープ制御装置２に、暗号・復号化回路１２を設けたので、上位装置１は、暗号・復号処理をしなくて済み、上位装置１の負担が軽減するとともに、入出力処理に暗号・復号機能を持たせなくて良いので、入出力処理が低下することもなく、複雑なプログラムの変更も必要なく、短期間で導入でき、プログラムによるエラー、障害等も発生せず、データ破壊を防止できる。

【００４５】しかも、暗号・復号化回路１２は、ハード構成のため、高速処理が可能であり、上位装置１を持たせずに実行できる。又、ライト時は、セットされた磁気テープカートリッジ４から暗号化の有無を判定するので、容易に暗号化、非暗号化の制御を可能とする。

【００４６】更に、リード時は、リードデータから、暗号データか否かを判定しているので、確実に判断できる。しかも、オペレータの設定により、暗号方法、暗号キーを設定できるので、数種の暗号・復号化が可能であり、ユーザーは、自己のコンピュータセンター特有の暗合・復号化方法を選択でき、より安全性が高い。

【００４７】又、圧縮、伸長を同時にできるため、ユーザーの要求に応じたデータ変換が可能となる。

(b) 他の実施例の説明

上述の実施例の他に、本発明は、次のような変形が可能である。

【００４８】①リード時に、リードデータから暗号データか否かを判定しているが、そのようなデータを持たない時は、磁気テープカートリッジ４の暗号センサ３０ａの出力により、判断しても良く、リードデータの分析結果と暗号センサ３０ａの出力のマッチングを取り、確認しても良い。

【００４９】②ライト時に、磁気テープカートリッジ４の暗号センサ３０ａの出力により、判断しているが、このようなセンサを持たない場合には、上位装置１で暗号化か否かが判るから、上位装置１からの命令により、暗号化するか否か制御しても良く、上位装置１のかかる命令と磁気テープカートリッジ４の暗号センサ３０ａの出力のマッチングをとり、磁気テープカートリッジ４の誤セットを検出しても良い。

【００５０】③又、リード時に、上位装置１はアクセスするファイルにより、暗号化されているか否かを判定できれば、上位装置１の命令により、復号するか否かを判断できる。

【００５１】④ライト時及びリード時の暗号・復号指示を、オペレーション設定部１１より行っても良い。

⑤外部記憶媒体を、磁気テープで説明したが、可換型の磁気ディスク・光ディスク、光カード、ＩＣメモリ等の可換型記憶媒体にも適用できる。

【００５２】以上、本発明を実施例により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【００５３】

【発明の効果】以上説明したように、本発明によれば、次の効果を奏する。

①外部記憶制御装置に、暗号・復号化回路を設けたので、暗号・復号化処理を外部記憶制御装置で自動的に実行できるため、上位装置の負担が軽減し、入出力処理の低下を防止できる。

【００５４】②上位装置の処理に変更を加える必要がないので、障害等の発生を防止でき、しかも短期間で導入できる。

③暗号・復号化回路が、専用のハード回路のため、高速処理が可能となり、上位装置１を待たせずに、暗号・復号化を実行でき、コンピュータシステムのセキュリティの向上を高速に実行できる。

【図面の簡単な説明】

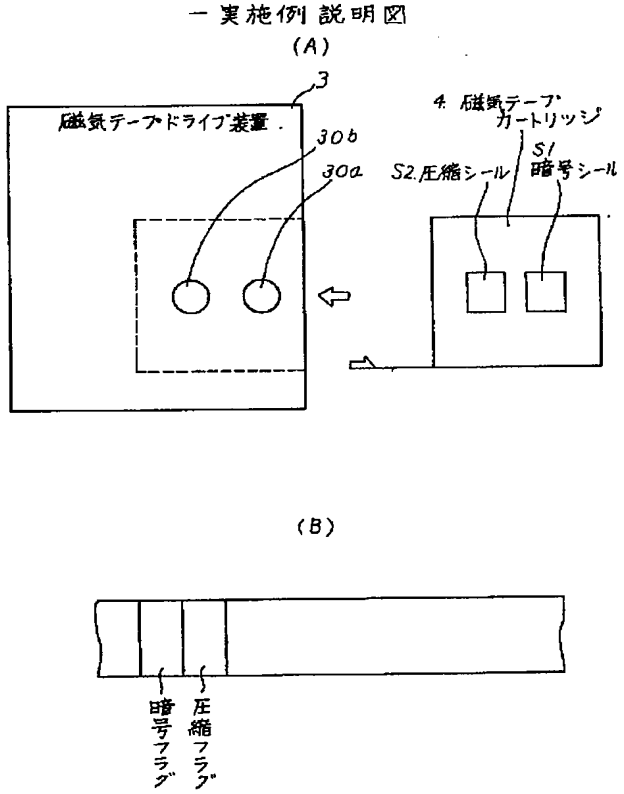
【図１】本発明の原理図である。

【図２】本発明の一実施例構成図である。

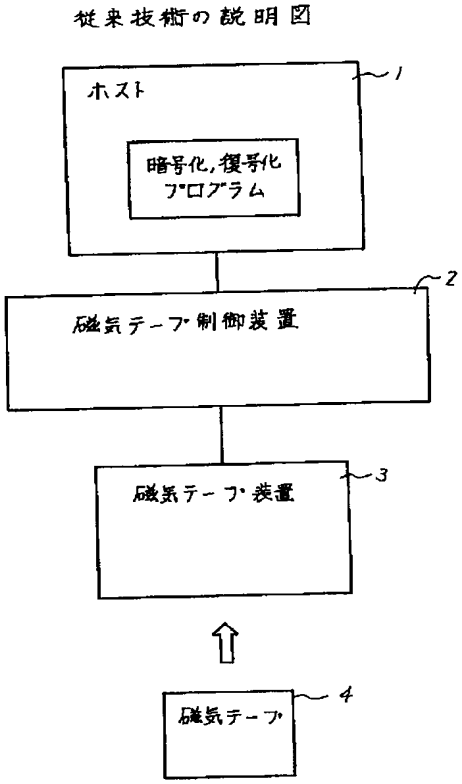
9　　10

【図３】本発明の一実施例説明図である。
【図４】従来技術の説明図である。
【符号の説明】
1　上位装置（ＣＰＵ）
2　外部記憶制御装置（磁気テープ制御装置）
3　外部記憶装置（磁気テープ装置）
4　可換型記憶媒体（磁気テープカートリッジ）
7　制御部
＊１０　チャネルインターフェース部
１１　オペレーション設定部
１２　暗号・復号化回路
１７　リードフォーマター部
１８　ライトフォーマター部
１９　デバイスインターフェース部
３０　暗号・圧縮テープ検出機構
＊

【図３】

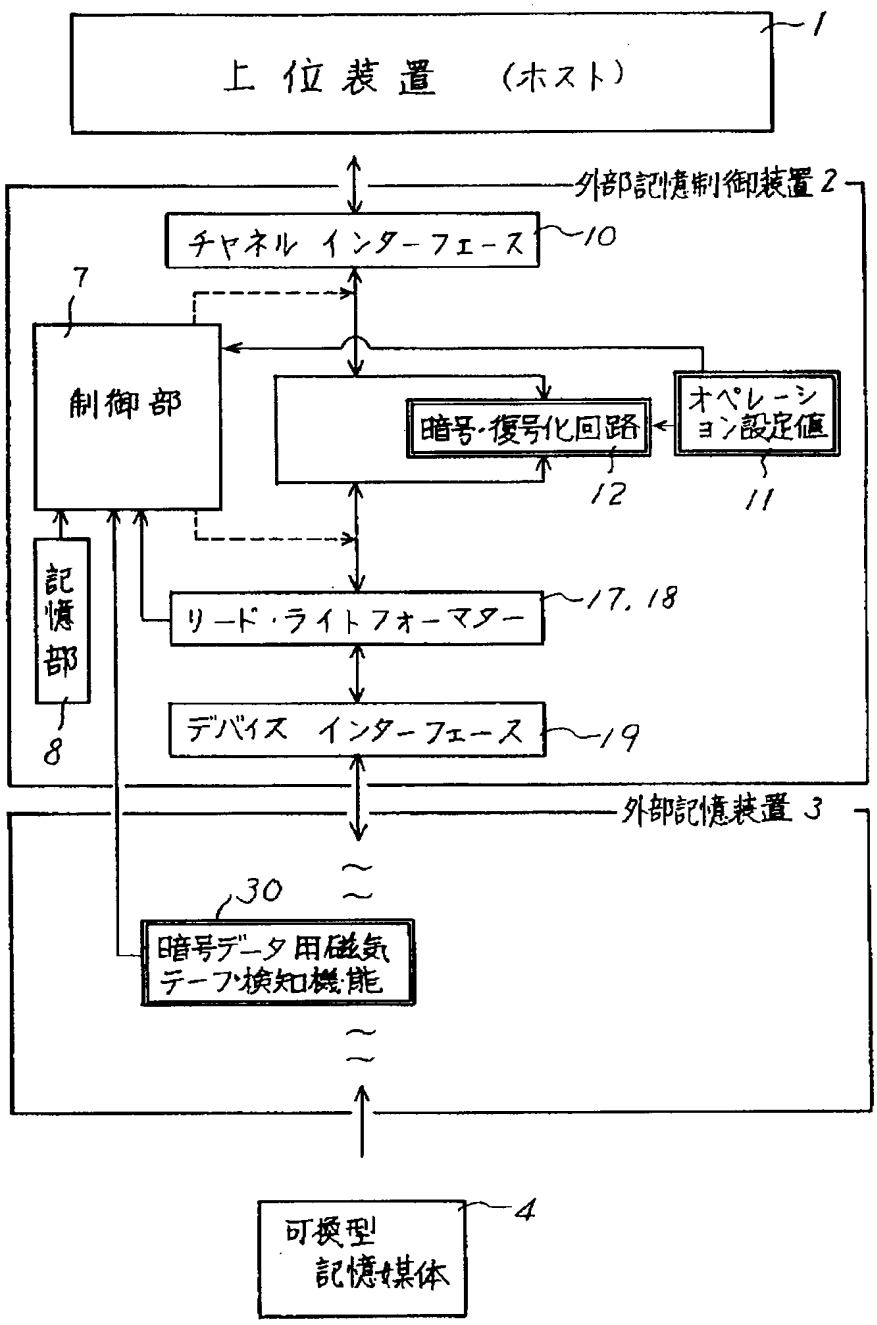


【図４】

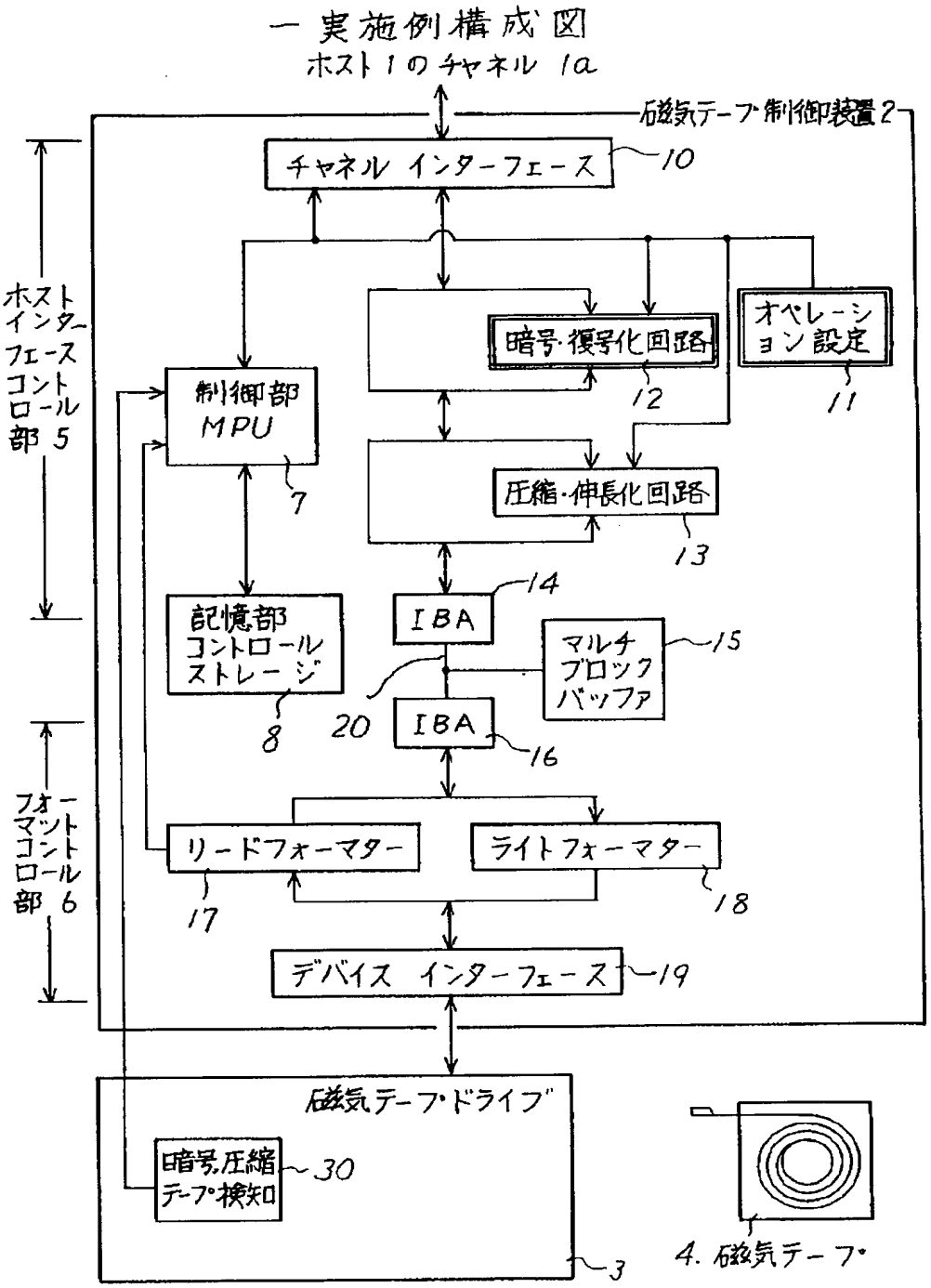


【図１】

本発明の原理図


上位装置　(ホスト)
1
外部記憶制御装置 2
チャネル インターフェース
10
7
制御部
暗号・復号化回路
12
オペレーション設定値
11
記憶部
8
リード・ライトフォーマター
17, 18
デバイス インターフェース
19
外部記憶装置 3
30
暗号データ用磁気テープ検知機能
可換型記憶媒体
4

【図２】


一実施例構成図
ホスト1のチャネル 1a
磁気テープ制御装置 2
チャネル インターフェース
10
ホスト
インター
フェース
コント
ロール
部 5
暗号・復号化回路
12
オペレーション設定
11
制御部
MPU
7
圧縮・伸長化回路
13
14
IBA
記憶部
コントロール
ストレージ
8
20
IBA
16
マルチ
ブロック
バッファ
15
フォー
マット
コント
ロール
部 6
リードフォーマター
17
ライトフォーマター
18
デバイス インターフェース
19
磁気テープドライブ
暗号圧縮
テープ検知
30
3
4. 磁気テープ